Mobile Application Security Testing (Android & IOS)

Ensure the security of your Android and iOS applications with comprehensive testing.

Contact Us

Mobile Application Security Testing (Android & iOS)

Ensure the security of your mobile applications with our comprehensive testing services designed to address varying levels of risk and exposure:

Automated Mobile Application Vulnerability Scanning

- Automated scans to detect common vulnerabilities in mobile applications.
- Price: €200 per application | Duration: 48 hours | Optional Kick-Off Meeting | Direct Submission of App Binary (APK/IPA).
- Receive a comprehensive report of detected vulnerabilities, analyzed by our team of experts with remediation advice.

Black-Box Mobile Application Penetration Testing

- Simulates attacks with no prior knowledge of the application's internal workings.
- Price: €400 per application | Duration: 72 hours | Optional Kick-Off Meeting | Direct Submission of App Binary (APK/IPA).
- External assessment of your mobile application, including manual and automated tests to identify security vulnerabilities, with a detailed report and actionable recommendations.

Gray-Box Mobile Application Penetration Testing

- Combines limited access (user credentials or low-level documentation) with penetration testing to uncover deeper vulnerabilities.
- Price: €200/24 hours | Duration: Based on Scope (Guidelines Provided) - Min 3 days | Mandatory Kick-Off Meeting.
- Leverage partial access to the application for thorough testing of business logic, APIs, and backend communications, with an in-depth report and mitigation steps.

Order Now

Explore Service Details

	Automated Vulnerability Scanning	Black-Box Penetration Testing	Gray-Box Penetration Testing
Prerequisites	APK/IPA Mobile Application	APK/IPA Mobile Application	APK/IPA Mobile Application, Credentials
Test Type	Automated	Automated and Manual	Automated and Manual with Internal Knowledge
Actions	Identify and Report vulnerabilities	Identify, Exploit and Report vulnerabilities	Identify, Exploit and Report vulnerabilities
Used Tools	MobSF, Burp Suite Scanner	MobSF, ADB, Frida, Drozer, Burp Suite	MobSF, ADB, Drozer, Frida, Burp Suite, APKTool, jadx, Ghidra
Covered Vulnerabilities	• Vulnerable and Outdated components • Insecure Data Storage • Weak Cryptography • Hardcoded Secrets • Insecure Communication	All the vulnerabilities from the Automated Vulnerability Scanning plus the following: • Insecure File Handling (e.g., exposing sensitive files, directory traversal) • Injection flaws (e.g., SQL, XSS, OS, NoSQL, LDAP, HTML, JSON, XPath, XML) • Security misconfigurations • Insecure direct object references • Server-side request forgery (SSRF) • Unvalidated redirects and forwards • XML External Entities (XXE)	All the vulnerabilities from the Automated Vulnerability Scanning and Black-Box Penetration Testing plus the following: • Authentication and Authorization Flaws • Business logic flaws • Design flaws • API Vulnerabilities (e.g., mass assignment, improper input validation) • Zero-day vulnerabilities • Privilege escalation • Insider threats • Complex application workflows

		- Design flaws	
Reporting	Comprehensive Report with Automated findings with expert review and remediation guidance.	Comprehensive Report with vulnerability details, exploit paths, risk assessment, and Remediation Recommendations.	Comprehensive Report with vulnerability details, exploit paths, risk assessment, and Remediation Recommendations.
Duration	48 hours	72 hours	Based in Scope (Determined in Kick-Off Call)
Price	**€200** Order Now	**€400** Order Now	**€200/24 hours (min 3 days)** Order Now

Step-by-Step Process

1. Order Service Request

The client orders a "Service Request" by completing the contact form, providing the details of the resources in scope, a brief project description, and contact information.

2. Scope Review & Kick-Off (if applicable)

We review the Service Request and, if necessary, schedule a 30-minute kick-off meeting to discuss the effort estimation, project timeline, and details regarding the in-scope resources. For Black-Box tests, we can proceed directly to the next step.

3. Contract and Payment

Once the details are agreed upon, we send the client a contract and invoice. After the contract is signed and payment is received, we begin the testing phase.

4. Testing Execution

Our expert team conducts a combination of automated and manual tests, simulating real-world attack scenarios to uncover vulnerabilities and assess security posture.

5. Report Delivery

Upon completion, you'll receive a comprehensive report detailing identified vulnerabilities, their severity levels, and actionable recommendations to enhance your security.

Subscribe to our newsletter

Email address

Your email address

Submit

Contact

office@ethicsec.com

Hours

Mon-Fri: 9am-5pm

Socials